나무위키

인터넷 프라이버시

최근 수정 시각: 2026-08-17 22:08:27

분류:프라이버시 | 인터넷 | 정보인권

검열 및 감시

[펼치기 · 접기]

목차

1. 개요
2. 인터넷 프라이버시의 침해 위험 요소
   2.1. 빅 데이터
   2.2. 검색 엔진
   2.3. 운영체제
   2.4. 웹 브라우저
   2.5. SNS
   2.6. 광고 및 추적 쿠키
   2.7. 사진
   2.8. 해킹
   2.9. 정부기관 또는 공권력
   2.10. 서비스 제공 업체
   2.11. 보안 플러그인 및 안티 치트
   2.12. ISP
   2.13. 물리적 방법
3. "숨길 게 없다면 걱정할 필요도 없다"에 관한 논쟁
   3.1. 프라이버시에 반하는 쪽
   3.2. 프라이버시를 중시하는 쪽
4. 위험을 줄이는 방법
   4.1. 검열과 감시
   4.2. 프라이버시 VS 익명성 VS 보안
   4.3. 익명과 가명
   4.4. 위협 모델링
   4.5. 검열로부터 자신을 보호하는 각종 팁
   4.6. 이외 각종 주의사항
      4.6.1. 기술적 주의사항
      4.6.2. 기타 주의사항
      4.6.3. 토어도 만능은 아니다
   4.7. 비밀번호
   4.8. 번역 서비스 이용
   4.9. 암호화 서비스 이용
   4.10. 프라이버시 메신저 이용
   4.11. SNS 이용 시
   4.12. 보안 강화
      4.12.1. 물리적 격리
   4.13. 검색엔진과 브라우저
5. 관련 사건
6. 관련 문서

1. 개요

인터넷 상에서의 프라이버시를 말한다. 데이터 프라이버시의 일종이며 인터넷이 발달하지 않았을 시절에는 대두되지 않았지만 전 세계적으로 인터넷 망이 발달하고 고도화되면서 세계적 이슈로 떠올랐다.

2. 인터넷 프라이버시의 침해 위험 요소

2.1. 빅 데이터

자세한 내용은 빅 데이터 프로세싱 문서의 5번 문단을 참고하십시오.

2.2. 검색 엔진

2.3. 운영체제

마이크로소프트의 Windows 10은 사용자의 사용 패턴 등 사생활 데이터를 매우 많이 수집한다. Windows 7부터 마이크로소프트 계정과 운영체제를 연동하게 되면서 더욱 심해졌다. 리눅스 배포판을 사용하면 완전히 정보를 지킬 수 있겠지만 그것이 어렵다면 W10Privacy 등의 툴을 이용하여 전송되는 정보를 최소화할 수 있다.

2.4. 웹 브라우저

일부 웹 브라우저는 사용자의 검색 기록을 무단으로 수집하기도 하였다.

2.5. SNS

전 세계인들이 자발적으로 트위터, 페이스북, 인스타그램, 유튜브 등 각종 sns나 미디어 사이트에 올린 자신에 관한 각종 정보(이름, 직업, 나이, 사진, 영상, 위치정보 등)들은 인터넷 프라이버시의 가장 큰 위협 중 하나다. 더구나 이것들은 다른 누군가가 몰래 정보를 수집한 것도 감시한 것도 아닌 스스로가 갖다 바친 것들이다.

일면식도 없는 제3자조차도 단순히 누군가의 페북이나 인스타 페이지를 보는 것만으로 그 사람이 누군지, 어떻게 생겼는지, 몇 살인지, 친구나 인맥 관계가 어떤지, 어느 학교를 다니는지, 직업이 무엇인지, 어디에서 뭘 먹고 돌아다니는지 알 수 있다. 인터넷상에서 가끔 이슈가 되는 이른바 '신상털기'가 가능한 것도 **소셜 네트워크 서비스** 때문이다.

2.6. 광고 및 추적 쿠키

인터넷 광고 업체는 타사의 웹 사이트에 추적 콘텐츠와 쿠키를 삽입하여 사용자의 검색 기록을 수집한다.

예를 들면 A라는 사이트에 B사의 광고가 실렸는데 B사의 추적 콘텐츠가 A사이트에서 활동한 기록까지 B사로 전송한다는 뜻이다.

2.7. 사진

sns와 달리 내가 아닌 다른 사람이 찍어 올린 사진에 자신의 모습이 담겨있을 수도 있다. 거의 대부분의 사람들이 디지털 카메라나 폰 카메라를 가지고 다니는 현재 생각보다 흔히 벌어지는 일이며 이 때문에 사진 취미가가 거리에서 사진을 찍다 보면 자신(또는 자신의 아이)이 나온 사진을 지워 달라고 요청하는 경우도 있다. 다른 예로는 구글 스트리트뷰가 있다. 실제로 구글 스트리트뷰에는 사람의 얼굴들이 모자이크 처리되기는 하지만 단순 행인뿐만 아니라 온갖 상황의 사진들이 찍혀 있어서 이슈가 되기도 했다. 구글 ceo인 에릭 슈미트는 일전에 스트리트 뷰에 자신의 집이 나오는 게 싫다면 이사를 가라고 말했을 정도로 크게 개의치 않다. 사진을 인터넷에 올릴 때 유의해야 할 사항 중 하나로 사진에 포함되어 있는 부가 정보로 해당 사진을 찍은 **위도와 경도**가 기록되어 있는 경우가 있다.[1] 서버에서 압축 등의 프로세싱을 거친다면 없어질지도 모르지만 해당 정보가 그대로 남은 채로 업로드되는 경우도 있다.

2.8. 해킹

해커들에 의한 해킹으로 피해가 발생할 수 있다. 소니 픽처스 이메일 해킹 사건과 아이클라우드 누드 사진 유출 사건, 뽀로로 극장판 컴퓨터 왕국 대모험방송 도중 야동 송출 사고 등이 있었다.

2.9. 정부기관 또는 공권력

가장 대표적인 예로는 대한민국/문화 검열과 미국의 NSA가 있다. 특히 NSA가 운영하는 프리즘은 에드워드 스노든의 폭로로 세상에 알려진 바 있다. 해당 기업에 대해 영장이 나오는 경우에도 기업은 서버를 내어 줄 수밖에 없다.

2.10. 서비스 제공 업체

서비스를 제공하는 기업들은 약관에 수집하는 개인정보들과 이용처 등을 명시하고 있다. 다만 대부분의 사람들이 귀찮아서 읽지도 않고 그냥 동의를 누를 뿐. 아니면 그 기업의 약관이 맘에 들지 않더라도 어쩔 수 없이 동의를 하고 서비스를 이용해야 하는 경우도 매우 많다. 구글의 데이터 수집이 마음에 들지 않지만 안드로이드 스마트폰을 쓰기 위해서는 어쩔 수 없이 구글 계정을 만들어야 한다. 안드로이드가 싫어서 iPhone을 쓴다고 해도 이번엔 Apple 계정을 만들어야 한다. 결국 스마트폰을 포기할 게 아니라면 구글이든 애플이든 계정을 만들고 그들이 원하는 내 정보들을 넘겨줘야 한다. ~~LineageOS를 사용하고 GApps를 설치하지 않으면 된다.~~

구글에서 제공하는 각종 서비스들은 매우 편리하다. 지메일부터 구글 캘린더, 구글 포토, 구글 드라이브, 구글 나우... 일례로 호텔이나 비행기를 예약해서 그 예약 메일이 자신이 사용하는 지메일로 오면 구글은 자동으로 캘린더에 해당 일정을 추가하고 호텔 위치도 표시해 준다. 그리고 자신이 평소 야구 경기를 자주 검색하고 결과를 확인한다면 나중엔 구글 나우는 알아서 야구 경기가 있던 날에 내가 궁금해할 만한 야구 경기의 결과를 띄워준다. 놀라울 정도로 편리한 건 사실이다.

물론 사람에 따라선 오히려 거부감을 느낄 수도 있을 것이다. 저 말은 구글은 알아서 내게 오는 모든 메일의 내용을 자동 스캔하고 모든 서핑 기록도 분석한다는 뜻이니까. 구글 드라이브도 마찬가지로 드라이브 상에 올라가는 모든 파일은 구글이 열람할 수 있다.[2] 이는 구글뿐만 아니라 원드라이브 등 다른 대부분의 클라우드 스토리지 서비스들도 마찬가지. 구글이 가장 영향력이 크고 가장 크게 세계적으로 이슈화가 되는 기업이기에 관련 이슈에서 많이 언급될 뿐이다. 구글 외에 다른 업체들도 정도의 차이가 있을 뿐 크게 다르지 않다.

2016년 8월엔 롯데홈쇼핑이 회원 2만 9천여 명의 개인정보를 고객 동의 없이 보험사에 돈을 받고 판 것이 🔗적발되었다.

2.11. 보안 플러그인 및 안티 치트

많은 보안 플러그인 및 게임 안티 치트는 보안 향상을 목적으로 사용자 정보를 수집하고 있다. 일반적인 백신이라면 삭제하면 그만이지만 보안 프로그램을 설치하지 않으면 서비스 제공 자체를 거부하는 경우가 많아 어쩔 수 없이 설치하는 경우가 대다수이다. 이들은 사용자 권한이나 관리자 권한보다 높은 커널 권한으로 실행되기 때문에 개인 파일이나 인터넷 검색 기록 등의 개인정보에 무리 없이 접근할 수 있다.

2.12. ISP

2.13. 물리적 방법

가장 단순 무식한 방법. 가장 가까운 예로는 주변 사람이나 애인이 휴대폰 훔쳐 보거나 미처 로그아웃하지 않은 웹사이트나 메일을 보는 방법이 있다. 이를 막기 위해 자리를 떠날 때마다 잠금을 해 놓거나 사생활 보호필름을 부착해야 한다.

암호학에서는 이런 방법을 사회공학의 일종으로 보거나 또는 단순하게 물리적 해킹이라고 한다.

3. "숨길 게 없다면 걱정할 필요도 없다"에 관한 논쟁

개인정보나 프라이버시 침해에 관한 얘기에서 가장 흔하게 나오는 말. 스마트폰을 통한 해킹이나 피싱에 대해서도 "니 폰 털어봤자 중요한 것도 없는데 왜 걱정?"이라든가 심지어 가입했던 사이트에서 주민번호가 유출되어도 "어차피 그거 털어도 할 수 있는 것도 없잖아?"라며 대수롭지 않게 생각하기도 한다. 서비스 제공 업체들에 의해 수집되는 메타 데이터들과 가입자들의 메일, 파일에 대한 접근에 대해서도 마찬가지다.

하지만 이걸 오프라인 세상으로 바꿔서 생각한다면 자신이 주고 받는 모든 우편과 택배들이 우체국 또는 택배사에 의해 중간에 개봉되어 확인된다고 해도 '난 숨길게 없으니까 그렇게 해도 괜찮아'라고 할 수 있을지, 누군가가 1년 365일 24시간 자신이 어디에 가든 무엇을 하든 뒤를 미행한다 해도 '난 죄진 게 없으니까 따라다녀도 괜찮아'라고 할 수 있을지 의문이다. 사생활의 비밀과 자유는 모든 사람의 기본적 권리이기 때문에 자신이 숨길 게 있느냐 없느냐와는 무관한 문제다. 본인은 괜찮더라도 상대방은 아닐 수 있고 나중에 맘이 바뀌었는데 상대가 본인과 가깝다고 해서 신상을 맘대로 공개하고 이후 관계를 끊어도 이러한 행위가 지속되면 어떻겠는가?

암호화 통신을 사용하는 사용자가 많아지면 많아질수록 통신을 분석하는데 더 큰 비용이 들어가기 때문에 굳이 필요하지 않더라도 사용하는 것이 좋다.

3.1. 프라이버시에 반하는 쪽

- CCTV 운영 프로그램이 매우 활발한 영국에서 사용하는 모토도 "If you've got nothing to hide, you've got nothing to fear"이다.
- 구글의 CEO인 에릭 슈밋은 🔗구글의 프라이버시 침해에 대한 얘기에서 "만약 당신이 남들이 모르기를 바라는 뭔가가 있다면 애초에 그런 행동을 하지 말았어야 한다"[3]고 말했다.
- 또, 에릭 슈밋은 스트리트 뷰에 자신의 집이 나오는 게 싫다면 이사를 가라고 말하기도 했다.
- 헨리 제임스는 그의 1888년작 소설 '반향'에서 "만약 이 사람들이 나쁜 짓을 했다면 스스로 부끄러워해야 할 것이고 그는 그들을 동정할 수 없었다. 하지만 만약 그들이 나쁜 짓을 하지 않았다면 다른 사람들이 알게 되는 것을 두고 이렇게 소란을 피울 필요는 없었다."[4]라고 했다.

3.2. 프라이버시를 중시하는 쪽

- 컴퓨터 보안 전문가 브루스 슈나이어는 "'보안 vs 프라이버시'의 문제가 아니라 '자유 vs 통제'의 문제"라고 했다.
- 에드워드 스노든은 "숨길게 없으니 프라이버시가 침해 되어도 상관없다는 사람은, 말할 게 없으니 표현의 자유가 없어도 된다고 말하는 것과 같다."[5]고 말했다.
- 미국의 배우 알렉스 윈터는 "숨길 것이 없으면 두려워할 것도 없다는 생각을 받아들이지 않는다. 사생활은 목적이 있다. 창문에 블라인드가 있고 욕실에 문이 있는 것도 바로 그 때문이다."[6]고 말했다.

4. 위험을 줄이는 방법

물론 이 세상에 위험을 없애는 완벽한 방법은 없지만 피해를 줄이는 것은 가능하다. 프라이버시를 지키기 위해서는 많은 지식이 필요하다.

4.1. 검열과 감시

많은 사람들이 정부의 차단·검열과 감시를 혼동하는 경향이 있는데 사실 차단하지 않아도 감시는 얼마든지 가능하다. 그냥 가만히 지켜보기만 하면 되는 거니까. DNS/SNI 암호화(유니콘https, 1.1.1.1 등)는 차단 회피용으로는 아주 좋지만 감시에 대해서는 유의미한 수준의 방어력을 제공해 주지 않는다. DNS와 SNI가 암호화되더라도 사용자가 어떤 IP 주소와 통신하는지는 숨겨지지 않기 때문이다. 네트워크 감시자는 그 IP주소를 보고 사용자가 어떤 사이트에 들어가는지를 알아낼 수 있다. 일단 이 부분은 편지로 비유하자면 편지봉투의 주소이고 편지 내용을 하나하나 감시하는 건 이미 물리적으로 불가능할 수준에 이르기는 했다.

🔗HTTPS 차단 우회방법 총정리🔗@, 🔗프라이버시, 추적방지를 위해서는 VPN이 아닌 토어를 써야 하는 이유🔗@

4.2. 프라이버시 VS 익명성 VS 보안

세 가지 말은 혼용되어 쓰이지만 조금씩 차이가 있다.

> Privacy is a state of being free from **observation**.
> 프라이버시란 **관찰**로부터 자유로운 상태를 말한다.
>
> Anonymity is a state of being free from **identification**.
> 익명성이란 **신원 확인**으로부터 자유로운 상태를 말한다.
>
> Security is a state of being free from **danger**.
> 보안이란 **위험**으로부터 자유로운 상태를 말한다.
>
> 🔗Privacy, security, and anonymity: What's the difference?
> 프라이버시는 **콘텐츠**를 숨기는 것이고, 익명성은 **신원**을 숨기는 것이다.
> 🔗How do you differentiate privacy and anonymity?

🔗한글 사이트로 설명
예를 들어 당신이 온라인 쇼핑몰에서 물건을 구매했다고 가정해 보자.
프라이버시: 당신이 무엇을 구매했는지 타인에게 알려주지 않는다.
익명: 구매자가 당신인지 타인에게 알려주지 않는다.
보안: 당신의 계좌를 해킹할 수 없게 막는다.

프라이버시와 익명성을 구분하는 예시로 Signal(메신저)를 들 수 있다. 시그널 메신저는 1대1 대화방과 단체 대화방 모두 종단간 암호화(E2EE)를 지원하므로 프라이버시는 보장되지만 메신저 사용 시 전화번호를 요구하므로 익명으로 구입한 가상번호로 가입하지 않는 이상 익명성은 보장되지 않는다.

토어 브라우저를 사용하면 아무도 당신이 방문하는 웹사이트를 볼 수 없으며(프라이버시), 아무도 당신의 브라우징 활동을 기반으로 당신을 식별할 수 없다(익명성). 그러나 토어를 포함한 어떤 브라우저를 사용하더라도 방문하는 웹사이트가 그 웹사이트 내에서 일어난 활동을 알 수 있으므로 완전한 프라이버시가 아니다.

보안은 이와 별개의 문제다. 만약 토어를 통해 바이러스 사이트에 접속하면 악성코드가 기기에 설치될 수도 있다.

4.3. 익명과 가명

- 익명성(Anonymity): 한 사람의 신원이 자신 이외의 모든 사람에게 알려지지 않은 상태.
- 익명연결(Anonymous connection): 연결의 출처(IP 주소/위치)를 발견하거나 식별자와 연결할 수 없는 대상 서버에 대한 연결이다.
- 가명성(Pseudonymity): 사람의 실명은 아니지만 일관된 식별자를 갖는 익명에 가까운 상태.
- 가명연결(Pseudonymous connection): 연결의 출처(IP 주소/위치)를 찾을 수 없지만 요청이 식별자와 연결될 수 있는 대상 서버에 대한 연결이다. 가명 식별자가 더 자주 감지될수록 이 가명을 실제 신원으로 추적하기가 더 쉬워진다.

인터넷상에서 익명 연결(Anonymous connection)이란 자신이 도달한 서버가 자신의 본래 IP 주소 혹은 위치를 알아낼

방도가 없으며, 그 외의 **다른 수단이나 식별 도구로도 자신을 특정할 수 없는 연결**을 말하고, 가명 연결(Pseudonymous connection)이란 자신이 도달한 서버가 본래 IP 주소 혹은 위치를 알아낼 방도는 없으나, 이 외의 **다른 수단이나 식별 도구로 자신을 어떻게든 특정할 수 있는 연결**을 말한다.

이상적인 세계에서는 토어 네트워크, 토어 브라우저, 컴퓨터 하드웨어, 물리적 보안, 이상적인 OS 등을 사용하여 완벽한 익명성을 보장할 수 있긴 하다. 이러한 개념적 유토피아에서는 유저가 뉴스 웹사이트에 접속하여 뉴스를 읽는다 하더라도, 그 뉴스 웹사이트나 ISP에서는 이 유저가 본인들의 서버에 연결을 했는지조차도 모를 수도 있다.

물론, 조금 더 현실적으로 다가가자면 이렇게까지 완벽한 보안과 프라이버시를 유지할 수 있는 유저는 사실상 없다. 예를 들어 만약 누군가가 토어 브라우저 대신 일반 파이어폭스로 토어 네트워크에 접속한다면 자신의 보안이나 프라이버시를 지키는 데 실패하는 것이다. 토어 네트워크를 통해 자신의 실제 IP 주소나 위치를 숨기는 것까지는 좋았지만, 일반적인 파이어폭스를 사용함으로서 쿠키 같은 식별 도구가 이러한 연결을 익명 연결(Anonymous connection)이 아닌 가명 연결(Pseudonymous connection)로 만들어 버리기 때문이다. 예시를 들자면, 어느 한 도착한 웹사이트는 [ID 111222333444를 가진 유저가 제목 A라는 영상을 B 시간 C 날짜에 시. 청한 다음, 제목 D라는 영상을 E시간 F날짜에 시청함] 이라는 로그를 저장하고 있을 수도 있다. 단순히 몇 번 시청한 것만으로 이 유저를 추적하기에는 굉장히 어렵겠지만, 시간이 지날수록 이러한 로그와 같은 정보들은 더욱 자세하고 복잡해지며, 언젠가는 이른바 '프로파일링'을 가능케 만든다. 이러한 프로파일링이 지속될수록 익명성이 떨어지고, 최악의 경우에는 익명의 베일을 벗기고 유저를 완전히 특정하게 될 수도 있다.

유저가 자신의 IP 주소나 위치를 숨기고 어느 웹사이트에 로그인한다고 해도 마찬가지이다. IP 주소를 숨긴다고 해도 로그인하게 된다면 자신의 익명(Anonymity)은 망가지고 가명(Pseudonymity)인채로 연결하게 되는 것이다. 가명으로 연결되었기 때문에, 계정 이름 등을 통해 현실의 자신을 특정하게 된다. 식별자는 사용자가 무엇을 썼을 때 로그인 및 로그아웃 날짜와 시간, 사용자가 쓴 내용과 대상, 사용된 IP 주소(Tor exit 릴레이 제외), 기록된 브라우저 핑거프린트 등 다양한 것이 될 수 있다.
익명이 되는 것은 어렵고 많은 지식이 필요하다.
🔗 익명과 가명의 차이점에 대하여
🔗 Tips on Remaining Anonymous

4.4. 위협 모델링

🔗 Threat Modeling🔗 @
🔗 위협 모델

보안, 개인 정보 보호 및 사용 편의성의 균형을 유지하는 것은 개인 정보 보호 과정에서 가장 먼저 직면하게 될 가장 어려운 작업 중 하나이다. 모든 것이 절충안이다. **더 안전한 것일수록 일반적으로 더 제한적이거나 불편하다.** 종종 사람들은 권장되는 도구의 문제가 너무 어려워서 사용을 시작할 수 없다는 것을 알게 된다.

사용 가능한 가장 안전한 도구를 사용하려면 사용 편의성을 크게 희생해야 한다. 그리고 그 때조차도, 그 무엇도 **완벽하게 안전하지 않다.** 보안은 높지만 완전한 보안은 아니다. 그것이 위협 모델이 중요한 이유이다.

위협 모델은 보안/개인 정보 보호에 가장 가능성이 높은 위협의 목록이다. 모든 공격으로부터 자신을 보호하는 것은 불가능하므로 **가장 가능성이 높은 위협에 집중**해야 한다. 컴퓨터 보안에서 위협은 개인 정보 및 보안을 유지하기 위한 노력을 저해할 수 있는 잠재적인 이벤트이다.

중요한 위협에 집중함으로써 필요한 보호 기능에 대한 생각을 좁혀 업무에 적합한 도구를 선택할 수 있다.

4.5. 검열로부터 자신을 보호하는 각종 팁

[펼치기 · 접기]

오류가 발생했습니다.

www.youtube.com에서 동영상을 시청하거나 브라우저에서 자바스크립트가 사용 중지된 경우 사용 설정하세요.

🔗 SecureDrop
🔗 SecureDrop Onion 사이트

검열로부터 스스로를 보호하는 것은 생각보다 쉽지 않다. 프라이버시와 관련된 정보를 얻기 위해서 이 문서와 Tor, 가상 사설망 문서를 참고할 수 있다. 이 정보글들이 내부고발자나 언론인 등 익명이 절실하게 필요한 사람들에게 도움이 되기를 바란다.

1. 항상 기본적으로 사이트를 불신한다는 전제 하에 이용하도록 한다.
2. 회사가 아니라 기술을 믿는다. 회사가 이용자 개인정보를 제공하지 않는다고 주장하는 것(예: VPN)과 기술적으로 개인정보를 제공하는 것 자체가 불가능한 것(예: 토어 브라우저) 사이에는 큰 차이가 있다. 말뿐인 보호를 믿지 말고 실제 기술적 보호만을 추구한다.
3. 가능한 토어 브라우저의 보안 레벨은 Safest로 설정하는 것이 좋다. 특히 Onion 사이트라면 무조건 Safest로 해야 한다. 다만 무리하게 Safest만 고집하다가 토어 브라우저 사용을 포기하지는 말고 그냥 Standard를 쓸 수도 있다. Safest를 쓰고 싶어도 제대로 이용 가능한 사이트가 거의 없어서 Standard를 쓸 수밖에 없는 경우가 많다.
4. 만약 토어 브라우저의 언어가 영어(en-US)가 아니라면 영어(en-US)로 변경한다. Tails OS나 Whonix의 경우 기본 설정이 영어(en-US)이므로 신경 쓰지 않아도 된다.
5. 좋은 비밀번호를 만든다. 랜덤으로 고른 단어 여러 개(6개 이상)를 랜덤으로 배열하여 만든 20자 이상의 비밀번호가 좋다. 단어를 선택할 땐 단어들 간에 서로 관련 없는, 그리고 나 자신과도 관련 없는 단어를 선택한다.[7] 각각의 단어 사이에는 반드시 공백이 있어야 한다. 띄어쓰기도 하나의 문자로 인식되므로 비밀번호에 띄어쓰기를 포함해도 된다. 랜덤한 문자나 사전에 없는 단어를 추가하여 비밀번호를 더 강력하게 만든다. 좋은 예시로 '종교사회학 광고주 갈!매기 도미니카 공소시효 까막@눈'(60자리)[8]을 들 수 있다. 국어사전을 쓸 때는 책에 지문이 남지 않도록 장갑을 쓴다.🔗 #,🔗 #,🔗 #,🔗 #
6. 사이트에서 함부로 링크를 클릭하지 않는다. 다운로드, 압축풀기, 실행도 마찬가지이다. 링크가 궁금하면 PC 토어 브라우저 Safest에서 확인한다.
7. 사이트에 회원가입 할 때 이름, 이메일, 주소, 전화번호 또는 기타 개인 정보를 제공했다면 해당 웹사이트에서는 더 이상 익명이 아니다. 예를 들어 네이버 뉴스에 악플을 달았다면 토어 브라우저를 썼다고 해도 가입할 때의 개인정보를 이용해 사용자를 특정할 수 있다. 네이버 메일이나 카카오 메일로 가입했다면 그 계정은 익명이 아니다. 일회용 전화번호와 일회용 메일을 이용한다. 회원가입시 메일 입력란에 아무렇게나 입력해도 중복만 아니라면 가입되는 경우(ex. qqqqq@wwww.com)가 있으니 반드시 확인해 본다. 절대로 네이버 메일, 다음 메일, 구글 메일로 가입하지 않는다.🔗 #
8. 단 한 번이라도 원래 IP로 활동한 계정은 더 이상 익명이 아님을 명심한다. 사이트 관리자는 마음만 먹으면 사이트에 접속해서 하는 모든 활동을 기록할 수 있다. 예를 들어 관리자는 사이트 접속, 회원가입, 로그인, 글 작성, 로그아웃, 사이트 나가기까지 무슨 IP로 활동했는지 모두 기록할 수 있다. 회원가입만 VPN이나 토어로 하고 글 작성은

원래 IP인 상태에서 했다면 쉽게 특정당한다. 너의 원래 IP로 글을 작성했다는 기록이 있기 때문이다. 단 한 번이라도 원래 IP로 로그인했다면 즉시 그 계정을 버리고 처음부터 새로 만들어야 한다.

9. 운영체제도 Windows 대신 Tails OS나 Whonix를 이용해야 한다. 모바일 토어브라우저는 PC 토어브라우저에 비해 익명성이 떨어지므로 되도록 PC 토어브라우저를 이용하는 것이 좋다. 특히 Onion 사이트는 스마트폰으로 접속하지 않는다.[9]
10. 토어 브라우저를 사용할 때에는 보안레벨과 브리지 설정 외에 다른 설정은 되도록 건드리지 않는다. 확장 프로그램도 되도록 설치하지 않는다.[10][11] 이는 핑거프린팅 때문이다. 사이트 운영자는 이용자의 브라우저 설정을 어느 정도 파악할 수 있다. 예를 들어 글씨 크기를 100으로 조정했다면 해당 이용자를 '여러 토어 이용자 중 한 명'에서 '글씨크기가 100인 토어 이용자'로 특정할 수 있는 식이다. 토어 설정을 건드릴수록 설정이 특이한 이용자로 특정하기가 쉬워진다. 다른 대부분의 토어 이용자들과 마찬가지로 초기 설정을 유지한다면 변경된 설정 내역을 바탕으로 개별 이용자를 구분하는 것이 좀 더 어려워진다. 토어는 모든 사람들이 미리 세팅된 설정을 똑같이 쓰기 때문에 핑거프린팅의 위협에서 다른 브라우저보다 안전하다.🔗#,🔗#,🔗#,🔗#
11. 인터넷이 끊긴 상태인 VM이나 Live mode 상태인 Whonix에서 파일을 열어보거나 압축 파일을 푸는 것이 좋다.
12. 의심되는 PDF 파일을 열 때는 토어 브라우저 Safest에서 PDF 파일을 열어서 읽는다. 더 나아가서 Whonix 라이브 모드의 토어 브라우저 Safest에서 PDF 파일을 읽거나, Qubes OS의 '신뢰하는 PDF로 변환'기능[12]과 Disposable VM을 사용하여 PDF 파일을 읽으면 더욱 좋다.🔗#
13. 의심되는 USB를 함부로 컴퓨터에 연결하지 않는다. 만약 궁금하다면 Tails OS를 켜고 인터넷 연결을 끊은 상태에서 컴퓨터에 USB를 연결한다. USB에 윈도우를 대상으로하는 악성코드를 심었다면 리눅스(Tails OS)에서는 아무 문제없어 보일 수 있으므로 방심하면 안 된다. 그러므로 USB는 Tails OS에서 데이터 완전 삭제과정을 거친 뒤에 윈도우에서 USB를 연결한다.
14. 리눅스에서 백신을 사용하지 않는다. 대신 Tails OS나 Whonix 라이브 모드를 이용한다.🔗#,🔗#,🔗#,🔗#
15. HDD와 SSD의 차이점을 알아보고 각각에 적합한 데이터 완전 삭제 방법에 대해 공부한다. HDD나 SSD를 일정 기간 써왔다면 암호화를 걸기전에 완전삭제를 한 번 거친다. 새로 HDD나 SSD를 구매했다면 바로 암호화해 준다. 참고로 암호화는 남들이 못 보게 하는 것이지 삭제를 못하게 하는 것은 아니므로 암호화된 채로 삭제해도 된다.🔗#[13][14][15][16],🔗#[17],🔗#[18][19],🔗#,🔗#,🔗#,🔗#,🔗#,🔗#,🔗#,🔗#,🔗#,🔗#
16. 데이터를 암호화하는 방법에 대해 공부한다. BitLocker와 VeraCrypt 각각의 장단점이 있으니 알아본다. BitLocker를 쓰든 Veracrypt를 쓰든 C드라이브 암호화는 필수이다. 새로 HDD나 SSD를 구매했다면 미루지 말고 바로 암호화해 준다. Veracrypt를 쓸 경우 설정 -> 단축키(Hot keys) -> '강제 모두 제거, 캐시 지우기, 끝내기'(Force Dismount All, Wipe Cache & Exit) 단축키를 설정해둔다. Tails OS와 Whonix가 리눅스이기 때문에 LUKS 사용법도 알아야 한다. 암호화 프로그램을 처음 사용해 보는 사람은 잘못하면 중요한 파일을 영영 찾을 수 없게 될 수도 있으니 암호화 프로그램의 사용법을 꼼꼼히 알아보고 중요한 파일은 따로 백업해두는 것이 좋다.🔗#,🔗#,🔗#,🔗#[20],🔗#,🔗#[21]
17. VeraCrypt의 히든 볼륨(Hidden Volume)에 대해 공부한다. VeraCrypt를 이용해 SD카드의 볼륨을 외부 볼륨 (노출용 볼륨)과 히든 볼륨으로 나눈 후 외부 볼륨에 적당한 파일을 넣어 두고 히든 볼륨에 중요한 파일을 보관한다. 만약 다른 사람이 SD카드의 암호화 해제를 요구하더라도 외부 볼륨만 풀어주고 안에 평범한 파일만 보여주면 된다. 항상 히든 볼륨의 존재는 발설하지 않도록 한다. 주의사항으로, 어떤 저장매체에 히든 볼륨을 만들었다면 해당 저장매체의 외부 볼륨에도 파일을 더 추가하지 않는 것이 좋다. 히든 볼륨의 영역을 덮어쓰면서 히든 볼륨을 파괴할 수 있기 때문이다. 히든 볼륨 보호 (Hidden Volume Protected)기능을 사용하면 히든 볼륨의 파괴를 막을 수 있지만 이 경우 SD 카드의 용량을 전부 채우는 방식으로 히든 볼륨의 존재를 쉽게 발견할 수 있으므로 [22] 히든 볼륨을 쓰는 의미가 없어진다. 따라서 히든 볼륨 보호 기능은 가능하면 사용하지 않을 것을 권장한다. 외부 볼륨과 히든 볼륨의 비밀번호는 반드시 달라야 한다. 만약 중국이나 북한같이 유죄추정의 원칙이 사회 전반에 통용되고 고무호스 암호분석(Rubber-hose cryptanalysis)을 대놓고 할 수 있는 국가에 살고 있다면 이런 국가에서는 정말로 히든볼륨이 없는 억울한 상황에서도 히든볼륨이 있다고 간주하고 죽을 때까지 고무호스 암호분석을 할 수 있으니 절대로 VeraCrypt를 쓰면 안 되고 무조건 히든 볼륨 같은 기능이 없는 BitLocker를 써야 한다.
18. 콜드 부트 어택(cold boot attack)에 대비한다. 컴퓨터 전원을 내렸더라도 몇 초 이내라면 급속 냉각 스프레이를 뿌려 메모리(RAM) 온도를 낮춘 다음 메모리 덤프를 떠서 메모리에 있던 개인키와 비밀번호를 복구해 암호화를 해제할 수 있기 때문이다. 메모리에 저장된 데이터가 완전히 휘발되기까지는 약 5분가량이 소요된다.🔗#,🔗#,🔗#
19. 스마트폰 보안을 신경 쓴다. 메시지 설정에서 MMS 자동 수신을 꺼둔다. 유심 비밀번호를 설정해 준다. 스마트폰은 BFU(Before First Unlock, 첫 잠금 해제 전)과 AFU(After First Unlock, 첫 잠금 해제 후) 상태로 나뉜다. 스마트폰 전원을 켜고 첫 잠금 해제를 한 이후 전원을 끄지 않았다면 AFU 상태이다. 스마트폰을 종료하거나 재부팅하면 BFU 상태가 된다. AFU 상태에서는 BFU에 비해 보안이 취약하여 잠금이 해제될 가능성이 높다. 그러므로 스마트폰 긴급 종료 방법을 알아둬야 한다. 안드로이드: 전원버튼+볼륨내림버튼 꾹 누름, 아이폰6s까지: 전원버튼+홈버튼 꾹 누름, 아이폰7: 전원버튼+볼륨내림버튼 꾹 누름, 아이폰8,X 이후: 볼륨버튼 위아래 한 번씩 짧게 누른 후 전원버튼 꾹 누름. 그리고 16자리 이상의 강력한 비밀번호를 사용해야 한다. 생체인식(지문인식, 홍채인식, 페이스아이디 등)을 해제한다. 구글이 활동기록을 수집하는 것을 줄이도록 설정[23]한다. FDE(Full Disk Encryption, 전체 디스크 암호화)와 FBE(File Based Encryption, 파일 기반 암호화)에 대해서도 알아본다. 참고로 픽셀폰에 그래핀OS를 쓰는 것이 가장 좋지만 편의성 등 여러 문제 때문에 대부분 안드로이드나 iOS 둘 중 하나를 쓴다.🔗#,🔗#,🔗#,🔗#[24]
20. Onion 사이트에서 스트리밍은 금물이다.🔗#
21. 토어 브라우저와 다른 브라우저를 동시에 사용하지 않는 것이 좋다.🔗#
22. 사진을 올릴 때 메타데이터[25][26][27]를 삭제해야 한다. ExifCleaner 같은 프로그램을 이용하여 사진의 메타데이터를 삭제할 수 있다. 스마트폰 화면을 캡처한 사진을 업로드할 때 상단바가 보이지 않도록 편집한다. 사진을 찍을 때 배경에 자신의 집바닥, 벽, 옷장, 물건 등이 나오지 않게 박스나 천 등으로 가리고 찍는다. 사진에 나온 손바닥과 지문을 분석할 수 있으니 조심한다. 가급적이면 애초에 사진이나 동영상을 올리지 않는 것이 좋다.🔗#[28],🔗#
23. 자기 신상을 떠벌리지 않는다. 침묵은 금이다. 프로파일링을 조심한다. 말투도 평소와 조금 다르게 한다.🔗#,🔗#
24. 글을 올릴 때는 웹사이트 글쓰는 창에 바로 타이핑하지 말고 메모장에 글을 쓴 뒤 복사(Ctrl+C)하고 글쓰는 창에 붙여넣기(Ctrl+V)하여 글을 올린다. 웹사이트에서 타이핑 습관, 특히 오타 습관을 수집하여 개인을 특정할 수도 있기 때문이다. 너무 짧은 글(ex. ㅇㅋ, ㄱㅅㄱㅅ 등)까지 메모장을 쓸 필요는 없지만 긴 글을 쓸 때는 메모장을 쓰는 것이 좋다.[29]
25. PGP (Pretty Good Privacy)와 GPG (Gnu Privacy Guard)에 대해 공부한다. 이메일은 토어 Safest에서 사용 가능한(다시 말해 자바스크립트 없이 쓸 수 있는) Onion 이메일을 사용한다. 다만 웬만해서는 Proton 메일 정도만 써도 무난하다.[30]🔗#,🔗#,🔗#[31][32],🔗#,🔗#,🔗#[33]
26. 모네로와 Zcash에 대해서 공부한다. 비트코인은 근본적으로 익명이 아니라는 사실을 명심한다.🔗#,🔗#
27. BASE64 등 인코딩에 대해 알아본다.🔗#
28. 파일을 압축하거나 압축 해제할 때 7-Zip을 사용한다. 7-Zip으로 7z뿐만 아니라 zip나 rar 등 다른 유형의 압축 파일도 풀 수 있다. 암호화 방식은 AES-256을 권장한다. 파일이름 암호화도 하면 좋다. 비밀번호는 강력해야 한다.🔗#,🔗#
29. 스테가노그래피(Steganography)에 대해 알아본다. 그 외에도 카이사르 암호 등 다양한 암호화 기술에 대해 알아본다.🔗#,🔗#
30. 파일을 공유할 때는 Onionshare를 사용하면 좋다.🔗#
31. 프라이버시에 좋은 메신저를 이용한다. 종단간 암호화(E2EE)는 서버에서 대화내용을 보지 못할 뿐 포렌식은 별개의 문제이므로 종단간 암호화 메신저를 사용해도 기기를 포렌식해서 대화내용을 복구할 수 있음을 명심한다. 최소한 카톡으로 중요한 얘기는 하지 않는 것을 권한다.🔗#[34][35][36],🔗#[37],🔗#[38],🔗#[39][40],🔗#,🔗#[41][42],🔗#,🔗#[43]
32. 각종 프로그램이 토어를 통해 연결되도록 설정한다. 프로그램의 프록시 설정에서 SOCKS5를 선택하고, 아이피를 127.0.0.1으로, 포트를 9150 또는 9050으로 설정한 뒤, 토어 브라우저를 켜두면 된다. 여기서 토어 브라우저는 Whonix의 Gateway 역할을 한다고 이해하면 된다. 텔레그램, Electrum 등등 다양한 프로그램에서 토어를 활용할 수 있다. 만약 프로그램 내에 프록시 설정이 없다면 Whonix의 Workstation에 프로그램을 설치하고 실행하면 된다. 모바일에서는 orbot을 이용해 다른 어플에서 토어 연결을 할 수 있다.🔗#,🔗#
33. 공유기 보안을 신경 쓴다. 와이파이 비밀번호와 관리자 비밀번호를 강력하게 설정한다. 만약 집에 손님을 자주 들

이거나 매장을 운영 중이라면 공유기의 게스트 와이파이 기능을 이용하여 외부인이 인터넷만 사용 가능하고 공유기 설정 페이지에는 접속하지 못하도록 한다. 게스트 와이파이의 비밀번호는 기존 와이파이의 비밀번호와 다르게 만든다. 통신사 공유기와 중국산 공유기는 사용하지 않는 것이 좋다. 🔗#,🔗#

34. ActiveX나 EXE보안프로그램은 프라이버시에 아주 해로우므로 윈도우에서 모두 삭제하고 가상머신의 윈도우에서만 설치한다.🔗#
35. HTTPS를 지원하지 않는 사이트[44]는 들어가지 않는다. 부득이 HTTP 페이지에서 로그인할 수밖에 없는 경우에는 해당 사이트의 아이디와 비밀번호를 다른 사이트와 다르게 설정해 놓음으로써 혹시 유출되더라도 해당 사이트에만 피해가 국한될 수 있도록 한다. 파일 다운로드도 하지 않는다.🔗#,🔗#[45],🔗#
36. 주소창에 주소를 입력할 때 번거롭더라도 https://를 입력해 준다. 예를 들어 구글은 'www.google.com'이라고 입력하지 말고 'https://www.google.com'이라고 입력하여 접속한다.🔗#
37. 웹캠을 포스트잇이나 스티커로 가린다. 혹시라도 해킹당했을 때 얼굴이 찍히지 않도록 하기 위해서이다.
38. Startpage의 Anonymous View 기능에 대해 알아본다.🔗#
39. 가입 시 약관을 꼼꼼히 읽는다. 필수만 체크하고 선택은 모두 체크해제한다. 귀찮다고 모두 체크하고 넘기지 않는다.
40. GetTor에 대해 알아본다.🔗#
41. 스마트폰을 쓸 때 가급적이면 어플보다는 브라우저를 사용한다.🔗#,🔗#
42. 지도 길찾기 서비스를 써야 할 때 출발지나 도착지를 자기 집 주소로 설정하지 않는다.
43. 오프라인 활동의 프라이버시 보호는 온라인에서보다 훨씬 더 어렵다는 점을 이해한다.🔗#,🔗#,🔗#,🔗#,🔗#,🔗#[46][47],🔗#[48],🔗#[49][50],🔗#[51],🔗#
44. 회사 컴퓨터로 허튼 생각하지 않는다. 회사 컴퓨터로 VPN이나 토어 브라우저를 이용하여 막아놓은 사이트[52]를 우회하려고 시도하지 않는다. 스마트폰을 할 때는 회사 와이파이보다는 데이터를 쓴다. 전산실 직원은 마음만 먹으면 뭐하는지 다 알 수 있다. 최악의 경우 해고당할 수도 있다.
45. 🔗VPN Gate 마이너 갤러리를 통해 정보를 얻는다. 한국어 정보는 부족하기 때문에 해외 커뮤니티도 보는 것이 좋다. 단 인터넷 정보는 신뢰성이 높지는 않으니 주의해야 한다.
46. 레딧의 🔗/r/privacy 서브레딧을 통해 정보를 얻는다.🔗예시
47. 🔗Hacker News를 통해 정보를 얻는다.🔗예시
48. 🔗4chan /g/ 아카이브 사이트를 통해 정보를 얻는다.🔗예시1[53]🔗예시2[54]
49. 🔗Privacy Guides를 참고한다.
50. 🔗프라이버시: 켜다를 참고한다.
51. 🔗AnarSec을 여러 번 정독한다.
52. 🔗The Nihilism OpSec Blog를 여러 번 정독한다.[55]
53. 🔗Navigating the Dark Web을 여러 번 정독한다.
54. 🔗The Hitchhiker's Guide to Online Anonymity를 여러 번 정독한다.[56]
55. 항상 교차검증한다. 인터넷 정보는 신뢰성이 낮다. 나무위키 또한 예외는 아니다.
56. 항상 공부한다. 공부는 아무리 많이 해도 언제나 모자라다.

4.6. 이외 각종 주의사항

🔗토어 브라우저 주의사항, 꿀팁, FAQ 정리🔗@
🔗토어 어니언onion 사이트 & 딥웹 FAQ🔗@

토어도 물론 완벽하진 않지만 주의사항을 잘 준수한다면 완벽에 가까운 정도의 익명성을 얻을 수 있다. 현재 이 문서에는 누락된 사항이 있을 수 있으니 관련 커뮤니티의 가이드를 함께 참조하는 것이 좋다. 한 가지 오해하지 말아야 하는 것은 토어에서 지켜야 한다는 주의사항 대부분은 토어를 사용하지 않을 때에도 적용된다는 것이다. 가장 대표적으로 자바스크립트는 마치 토어 브라우저에서만 사용하면 안 되는 위험한 플러그인으로 취급받지만 자바스크립트는 웹에 사용되는 프로그래밍 언어중 하나일 뿐으로 상당수의 웹사이트들이 자바스크립트를 사용하고 있다. 실제로 자바스크립트를 이용한 공격이 이루어지는 것은 사실이지만 이는 어디까지나 스크립트가 브라우저의 취약점을 노린 것이지 토어를 사용했다고 멀쩡한 스크립트가 갑자기 악성스크립트로 변하는 것은 아니다. 자바스크립트를 제어하는 것은 파이어폭스나 브레이브 같은 다른 브라우저에서도 보안성을 높이고 추적기를 차단하기 위해 해야 하는 상식이다.

4.6.1. 기술적 주의사항

- 토어 브라우저 번들만 사용
  기본 토어 브라우저 이외의 클라이언트를 사용하기 전에 본인이 그 클라이언트에 대해 완벽하게 이해하고 있는지 점검해야 한다. 잘 모르면 토어 인증을 받은 클라이언트만 사용하는 것이 좋다. 웹 브라우저의 인증 여부는 🔗여기[57]에서 확인할 수 있다.
- 암호화 프로토콜 사용
  출구 노드와 서버 사이에는 암호화가 되지 않아 통신을 가로챌 가능성이 있다. 되도록 HTTPS나 SMTP over SSL을 사용하는 것이 좋다.
- 플러그인 비활성화
  JavaScript 등의 플러그인은 토어 규격 이외의 방법으로 데이터를 전송하는 경우가 있으니 웬만하면 토어 Browser Bundle[58]를 통해 실행하자. 플래시나 개인정보 노출 가능성이 있는 옵션이 모두 꺼져 있다. 플래시를 보고 싶다면 🔗플래시 구동하는 방법[59]을 써야 한다.

4.6.2. 기타 주의사항

- 신원정보 숨기기
  토어 네트워크가 기술적 측면에서 익명성이 아무리 높다고 하더라도 스스로 신원정보를 드러내면 말짱 꽝이다. 토어 네트워크에서 표면 웹의 계정 또는 이메일, 닉네임 등을 이용하면 추적당한다.[60] 아이디와 비밀번호 모두 표면 웹에서 쓰지 않는 것으로 설정해야 한다. 신원을 추정할 수 있는 정보를 남기는 것도 좋지 못하다. 당연히 토어 네트워크로 기존에 쓰던 표면 웹 계정에 로그인하는 것도 좋지 못하다.[61] 최상위 도메인이 onion으로 끝난다면 익명성을 유지할 수 있지만, HTTP를 지원하거나 kr이나 .com 으로 끝나는 일반 면웹 사이트들은 토어를 사용하더라도 익명성이 깨질 수 있다.
- P2P 사용 자제하기
  토어 프로젝트 측에서는 비트토렌트와 같은 P2P를 토어를 통해서 이용하는 것은 위험한 데다 민폐라고 경고하고 있다. 토어 네트워크 상의 트래픽 여유는 전 세계 토어 이용자들 모두가 풍족하게 이용할 수 있을 만큼 여유롭지 않기 때문에 ~~겨우 야동 따위를 받으려고~~ 정말 필요한 이용자에게 피해를 주기 때문에 민폐이며, 이런 도의적 명분 외에도 P2P의 개념상 어쩔 수 없는 기술적 한계[62]도 있는데 첫 번째 문제로는 강제로 프록시를 설정하더라도 프로토콜의 차이로 제대로 먹히지 않거나 혹은 애초에 우회하도록 설계되어 있다는 점, 그리고 두 번째 문제로는 패킷 자체에 IP정보가 포함되기 때문에 토어의 프록시 빵빵이를 타더라도 패킷의 출처가 노출될 수밖에 없어 의미가 없다는 점이 있다. 토어와 기타 익명 프로그램들의 목적은 국가나 기관의 검열에서 벗어나 사람들이 자유로운 사상과 정보의 교류를 할 수 있도록 하는 것이지 리벤지 포르노나 아동 포르노를 공유하는 것이 아니다.[63]
  토어는 TCP를 쓰지만 토렌트는 UDP를 쓰기 때문에 **토어를 토렌트의 IP 주소 우회용으로는 쓸 수 없다.** 거기다가 일부 토렌트 프로그램은 패킷에 최초 IP 주소를 넣어서 전송하므로 이런 토렌트 소프트웨어를 사용할 경우 우회해도 소용없다.🔗#,🔗#,🔗#[64][65]
  정 쓰고 싶으면 P2P 프로토콜 자체에 토어 유사기술을 접목하려는 시도들이 있으므로 🔗정식으로 지원하는 Tribler 등을 쓰자. 22번째 댓글부터 보면 알겠지만 아직 사용자가 적어서 높은 익명성으로는 기존 토렌트만큼의 속도를 내기가 힘들다. 그렇다고 높은 속도로 설정하면 기존 토렌트 방식으로도 접속하므로 익명성이 떨어진다. 그리고 클라이언트 프로그램 자체도 여러 편의성이나 자잘한 안정성 면에서 비트토렌트나 뮤토렌트등의 메이져 클라이언트들에 비해 떨어지는 편이다.

만약 파일 공유를 하고 싶다면 Onionshare를 쓰는 방법도 있다. OnionShare는 토어 네트워크를 사용하여 안전하게 익명으로 파일을 공유하는 오픈소스 프로그램이다. 단 속도가 많이 느린 것은 감안해야 한다. 그리고 PC가 꺼지면 공유가 끊기기 때문에 24시간 파일을 공유하려면 PC를 24시간 켜놔야 한다는 것도 단점이다. 참고로 채팅 기능이 있기는한데 텍스트만 되고 이미지 업로드조차 안된다.

- 구글 접속하지 않기

  구글은 본인들도 밝히고 있듯이 개인정보를 수집한다. 토어는 접속 시작 시 DuckDuckGo로 연결된다.[66] 구글의 사이트인 유튜브에도 들어가지 않아야 한다. 유튜브 영상을 보고 싶으면 invidious라는 프로젝트를 통해서 볼 수도 있다. 구글의 검색 엔진을 사용하고 싶다면 Startpage를 사용한다.

- 휴대전화 번호 입력하지 않기
  휴대전화 번호도 개인정보이다.

- HTTP 사용과 같은 암호화되지 않은 정보 보내지 않기
  HTTPS를 사용해야 한다.

- 토어에서 만든 계정은 토어에서만 사용하기
  어떤 브라우저를 통해 어떤 계정이 접속했는지 해당 사이트에서 계정 기록을 수집한다. 이 계정 기록을 대조하여 사용자의 신원을 추적할 수 있다. 반대로 토어가 아닌 곳에서 만든 계정도 토어에서 사용하면 안 된다.

- 되도록 Windows에서 사용 자제
  Windows 버전도 있으나 보안이 약하다. Linux에서 사용을 권장한다.

- 보안 단계를 최대한 높이기
  다크웹 등을 접속할 시 자바스크립트가 비활성화된 safest 단계를 사용하는 것이 좋다. 참조

- 집에서 exit relay 설정은 피하기
  자원봉사 목적으로 tor relay를 집에서 운영할 경우 exit relay로 설정하지 않도록 주의한다. 일반적인 릴레이와 달리 암호화되지 않은 트래픽이 최종적으로 당신의 IP로 서버와 통신하게 되므로 법적인 문제가 생길 수 있으며, Tor의 Exit node 목록은 투명하게 공개돼 있기 때문에, 다양한 서비스 제공자들이 당신의 IP를 차단하는 등 다양한 제약이 생길 수 있다.

4.6.3. 토어도 만능은 아니다

주의사항을 모두 준수하고 최대한 익명으로 활동하려고 노력하고 토어 내부 네트워크에서만 활동해도 수사기관의 수사망을 완전히 빠져나갈 수 없다. 토어 프로젝트 측에서는 주의사항을 준수하여도 NSA의 기술력으로는 추적이 가능할지도 모른다고 경고했다. **NSA가 어떤 기술을 들고 있는지는 기밀이지만 NSA가 세계 최고의 암호 전문 정보기관이라는 건 거의 모든 보안전문가가 인정한다.** 토어 프로젝트도 익명성 보장을 위해 개선하고 있지만 NSA 정도 되는 초강대국 정보기관은 이미 그런 것쯤이야 뚫을 수 있는 기술력이 있을지도 모를 노릇이다. 실제로 FBI에서 몇 년에 걸쳐 궁리한 끝에 토어 브라우저 이용자에게 해킹툴을 다운로드하게 해 역추적한 사례가 있다.[67] 마약, 살인, 테러, 국가안보 위협, 아동 포르노 같은 쪽에는 국제적인 공조가 행해지고 있으므로 절대 완전범죄가 될 수 없다.

특히 한국에서는 토어 자체가 아닌 인터넷 해킹, 제품추적, CCTV 녹화, 통신 도감청, 물리적 압수수색[68] 등의 방식을 보조적으로 활용하여 수사해 들어갈 수 있다. 수사는 정보기만을 이용하는 것이 아니다. 토어나 해외 VPN은 국제공조와 압수수색영장 없이는 잡기 힘들지만 프록시 서버나 국내 VPN 등의 평범한 추적 회피 수단은 한국의 사이버수사대의 능력만으로 추적과 체포가 가능하다. 몇 가지 방안을 세워 놓은 나무위키도 예외는 아니다. 대표적인 예가 현금추적이다. 다만, 2024년 9월까지만 해도 실명사이트 로그인 등의 멍청한 짓을 하지 않은 경우 정상적인 IP추적으로 Tor 사용자를 검거한 사례는 단 한 건도 존재하지 않았다.

그러나 2024년 9월, 독일 당국이 전통적인 트래픽 상관관계 분석(traffic correlation)을 통해 한 Tor 사용자(아동 성범죄 관련 사이트 핵심 인물)를 특정한 사실이 알려졌다 관련 기사.[69] 원래 토어는 국가 단위, 혹은 여러 ISP 단위의 공격에 취약할 수 있음이 알려져 있었지만, 실제로 그런 공격이 가능함이 사례를 통해 입증된 것이다.

요점만 말하자면 경찰 입장에서는 사소하기 짝이 없는 단순 명예훼손/모욕죄 등에서는 몇 년 단위로 한 대상만을 노리는 정말 악질적인 경우가 아니라면 위의 주의사항만을 잘 지키면 국제공조 없이[70] 경찰이 신원을 특정할 수 있는 방법이 없어 수사가 성립조차 되지 않아 안전하지만[71] 아동 성범죄, 살인청부, 테러 모의 같은 죄질이 명예훼손이나 모욕 따위와는 비교할 수도 없는 악질 중죄와 더불어 불법이 아닌 나라가 없는 정도의 범죄를 저지르는 수준이라면 수사기관이 온갖 방법을 동원해 혈안이 되어 잡으려 할 테니 **토어고 VPN이고 뭐고 간에 잡힐 가능성이 높다.** 왜냐하면 오프라인에서 **아동 실종**접수만 받아도 장소의 경우의 수가 상당히 줄어들기 때문이다. **아동이 실종된 지역 + 수상하게 자주 바뀌는 VPN을 쓰는 집안**이면 사이트 운영자를 특정하는 것은 순식간이다. 간단한 예시로 인터넷 기법뿐만이 아니라 세무조사로도 (위험한 범죄가 공짜로 일어날 일은 없으니) 어느 정도 특정이 가능하다. 전 세계 경찰들은 바보가 아니다.

4.7. 비밀번호

자세한 내용은 비밀번호 문서를 참고하십시오.

암호(비밀번호)

비밀번호를 만들 때는 추측하기 쉬운 생일, 애완동물 이름, 전화번호 등을 포함하지 않는다.[72] 입력 사이트계정에 로그인할 때 2단계 인증을 하도록 설정하는 것도 좋다. 서비스 이용을 다 끝냈으면 반드시 로그아웃한다. 휴대폰이나 노트북에도 비밀번호를 설정하여 분실이나 도난 시를 대비한다.

4.8. 번역 서비스 이용

SimplyTranslate 등 여러 사이트를 통해 외국어를 번역할 수 있다. 가급적 국내 사이트인 파파고는 쓰지 않는 것이 좋다.

SimplyTranslate
일반 주소: https://simplytranslate.org/
Onion 주소: http://xxtbwyb5z5bdvy2f6l2yquu5qilgkjeewno4qfknvb3lkg3nmoklitid.onion/
I2P 주소: http://mmiyv57bfhgc7p4pipk7jjqv5meuz5rjijoviquplvhxl3v7aoba.b32.i2p/

4.9. 암호화 서비스 이용

암호화
메세지나 파일을 평문으로 전송, 보관하지 않고 암호화해서 전송, 보관한다. 암호화를 사용한다면 해킹으로부터 안전하고, 기업들이 자신의 데이터나 정보를 팔아넘기는 걸 방지할 수 있다.[73]

기존의 서비스들을 대체할 수 있는 것들로는 메신저로는 텔레그램의 비밀채팅[74], 카카오톡 비밀채팅, 시그널, 슈어스팟, Cryptocat 등이 있고 메일 서비스로는 Ghostmail, 오픈메일박스, Tuta, ProtonMail, Riseup 등이 있다. 클라우드 스토리지 서비스에는 Backblaze, MEGA, Spideroak, Tresorit, Peerio 등이 있다. 이들 서비스들은 각자 나름의 방식으로 암호화 서비스를 제공하고 있으니 살펴보고 자신이 원하는 것을 선택하면 된다.

만약 이런 서비스들도 못 믿겠다면 자신이 직접 암호화해서 사용하는 방법도 있다. OpenPGP나 AES 등을 이용한 암호화 프로그램들은 오픈소스로 이미 많이 공개되어 있다. 왜냐면 보안 전문가들도 얘기하듯이 인터넷상에서 100% 안전한 것이란 없다. 텔레그램은 보안에 의문을 제기하는 전문가들이 있으며, 많은 서비스 업체들이 '자신들조차도 고객들의 데이터를 보지 **못**한다'고 주장하며 홍보하지만 실제로는 그렇지 않은 경우도 많다. 암호화 이메일 서비스를 제공하던 Hushmail은 이미 고객들 뒤통수를 친 바 있다.[75] NSA 기밀자료 폭로사건으로 유명한 Lavabit도 비슷한 설계적 결함이 있었다.[76]

4.10. 프라이버시 메신저 이용

고려한 사항은 다음과 같다.

- 메신저 프로그램 설정 내에서 Tor 네트워크로만 연결하도록 설정할 수 없는 메신저는 Signal을 제외하고 모두 뺐다.
- 메신저 프로그램 내에서 설정을 따로 해야 Tor 네트워크로만 연결되는 메신저는 모두 뺐다.
- Tor 네트워크가 아닌 다른 익명 네트워크를 사용하는 메신저는 모두 뺐다.

프라이버시와 익명성을 위한 메신저는 아래의 요소를 충족해야 한다.

- E2EE: 모든 대화는 종단간 암호화(End to End Encryption, E2EE)된다. 이를 위해서 메신저 프로그램 내에서 설정을 따로 만지지 않아도 된다.
- Tor: 모든 대화는 Tor 네트워크를 통해서 오고 간다. 이를 위해서 메신저 프로그램 내에서 설정을 따로 만지지 않아도 된다.

Signal Messenger

웹사이트	https://signal.org/
충족하는 요소	E2EE
주의할 점	Signal은 전화번호를 요구하므로 익명이 아니다. 대화 내용이 암호화되는 메신저를 원할 때 사용한다.

Briar Messenger

웹사이트	https://briarproject.org/
충족하는 요소	E2EE, Tor
주의할 점	Briar는 모든 대화가 E2EE이고 Tor 네트워크를 통하지만 익명은 아니다.# 대화 내용이 암호화되고 대화의 메타데이터 유출을 줄이는 메신저를 원할 때 사용한다.

Cwtch Messenger

웹사이트	https://cwtch.im/
충족하는 요소	E2EE, Tor

OnionShare(채팅 기능)

웹사이트	https://onionshare.org/
충족하는 요소	E2EE, Tor

자신의 상황에 따라서 적합한 메신저를 선택하면 된다.

4.11. SNS 이용 시

자세한 내용은 소셜 네트워크 서비스/비판 문서의 2.2.2번 문단을 참고하십시오.

꼭 써야만 한다면 친구들만 볼 수 있도록 모든 포스트와 정보를 친구 공개로 해놓자. 전화번호나 집 주소 등의 민감한 정보는 아예 올리지 않는 게 좋다. 사진을 올릴 때도 풍경을 통해 거주지를 특정하기 쉬운 사진을 올리는 것은 좋지 않다.

4.12. 보안 강화

컴퓨터나 스마트폰의 운영체제를 최신으로 업데이트하고 윈도우 컴퓨터는 UAC가 작동 중인지 확인하고 안드로이드나 iOS는 앱에 필요 이상의 접근 권한을 허용했는지 확인해야 한다.

보안에 취약한 브라우저보다는 보안성이 높은 브라우저를 이용하고 웹 탐색 시 사용하는 브라우저와 플래시 등을 최신으로 업데이트해야 한다. 실제로 악성코드 중 일부는 이들의 취약점을 이용해 침투하기도 한다.

4.12.1. 물리적 격리

민감한 정보는 인터넷에 올리지 말고 외장 하드디스크 같은 콜드 스토리지에 담아 필요할 때만 꺼내 쓰는 방식을 쓰면 인터넷상의 누군가가 볼 수 있는 위험성을 원천 차단할 수 있다.

종이에 보안 정보를 따로 옮겨서 안 보이는 곳에 숨기는 것도 좋은 방법이다. 아예 금고에 넣거나 이것도 못 미덥다면 자신만의 암호를 만들어 단어나 의미를 재조합하면 매우 효과적이다. 당연하지만 보안 정보가 특정 금고 안에 있다는 사실을 누설하지 않는 것이 중요하다.

4.13. 검색엔진과 브라우저

유저 정보를 저장하지 않는 검색엔진을 사용한다. 예를 들면 덕덕고, Startpage 등.

브라우저는 Firefox 같이 추적 콘텐츠를 차단하는 기능이 있는 브라우저를 사용하고 검증된 광고 차단 플러그인을 설치하여 검색 정보를 수집하는 광고 콘텐츠를 차단하는 것이 필요하다.

5. 관련 사건

- 패프닝
- NSA 기밀자료 폭로사건
- 개인 정보 유출 사태
- 소니 픽처스 이메일 해킹 사건
- 박근혜 정부 카카오톡 사찰 논란
- 여성가족부 불법촬영물 오픈채팅방 단속 논란

6. 관련 문서

- 다크 웹
- Tor
- I2P
- Hyphanet
- GNUnet
- 가상 사설망
- Tails OS
- Whonix
- GrapheneOS
- PGP
- Cwtch(메신저)
- 모네로
- Zcash
- KeePassXC
- TLS 핑거프린팅
- VeraCrypt
- Mullvad Browser
- LibreWolf
- IronFox
- Syndie
- 야한 동영상/좋은 은폐 방법
- 프라이버시
- 잊힐 권리
- 빅 브라더
- 빅 데이터
- 정보보호
- 백 도어
- 유해매체 필터링 소프트웨어[77]

---

[1] 휴대폰에서 사진을 찍은 위치를 알려주는 경우가 있는데 이 사진이 휴대폰 밖으로 나가더라도 해당 정보를 알아낼 수 있다는 소리다.

[2] 자신이 구글의 거의 모든 서비스들을 이용하고 계정에서 별도의 비활성화 설정을 해놓지 않았다고 가정하면 구글의 서버에는 당신의 메일부터 구글 검색 기록, 유튜브 영상 시청 기록, 스마트폰 GPS를 통한 당신의 날짜별 시간별 이동 기록, 구글 드라이브와 구글 포토에 올라가 있는 당신이 찍은 사진, 문서, 구글 캘린더의 당신 일정, 연락처에 저장된 인맥, 구글 뉴스에서 당신이 읽은 기사 기록 등등 엄청난 양의 데이터 *원자재*들이 있으며 만약 이 원자재들을 가공하고 종합한다면 거기서 얻어 낼 수 있는 정보들은 가히 일반인들의 상상을 초월한다.

[3] "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"

[4] "If these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing.", 국내 미출판

[5] "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothong to say."

[6] "[he doesn't] accept the idea that if we have nothing to hide we have nothing to fear. Privacy serves a purpose. It's why we have blinds on our windows and a door on our bathroom."

[7] 예를 들어 '김영삼 김대중 노무현 이명박 박근혜 문재인'은 명목상으로는 6단어로 된 비밀번호이지만 실질적으로는 랜덤하게 고른 6개의 단어에 비해 추측해 내기 훨씬 쉬울 것임을 알 수 있다. 자기의 생년월일이나 출신 학교나 출신 동네 이름을 넣는다거나, 자기가 소중히 여기는 사람이나 동물이나 가치관의 이름을 넣는다거나, 자신의 직업상 자주 접하게 되는 개념 또는 사람의 이름을 넣는다거나 하는 것도 비밀번호의 추측 가능성을 증대시키는 요인이 된다.

[8] 해당 비밀번호에서 '갈!매기'와 '까막@눈'은 사전 공격(Dictionary Attack)을 방어하는 역할을 한다.

[9] 물론 모바일 토어가 PC 토어보다 못하지 크롬보다는 훨씬 낫다.

[10] 히토미 같이 악성광고가 지나치게 많은 사이트는 ublock origin을 설치해서 사용해도 딱히 큰 문제없다. 그러나 Onion 사이트에 접속하는 것이 목적이라면 되도록 처음 토어 브라우저를 열었을 때의 상태를 그대로 놔두는 것이 좋다.

[11] 다만 Tails OS의 토어 브라우저에 설치되어 있는 ublock origin을 일부러 삭제할 필요는 없다. 핵심은 처음 토어를 열었을 때의 상태를 그대로 놔두는 것이다.

[12] 참고로 DangerZone 프로그램이 이에 영감을 받아 만들어졌다. 단 DangerZone은 완전히 격리되어 있는 구조는 아니므로 방심은 절대 금물이다.🔗#

[13] 만약 부팅 관련 문제 때문에 Tails OS를 쓸 수 없는 경우 우분투나 리눅스민트 등 다른 리눅스로 시도해 본다. 그리고 데이터 완전 삭제를 목적으로 Tails OS를 이용할 경우, 바로 Start Tails 클릭하지 말고 Additional Settings 항목에 있는 '+'버튼을 눌러 Administration Password를 정해 준 뒤 Start Tails를 클릭한다.

[14] SSD의 랜덤데이터 덮어쓰기에서, dd if=/dev/urandom of=/dev/??? bs=4M status=progress 맨앞에 sudo를 추가해야 한다. 다시 말해 sudo dd if=/dev/urandom of=/dev/??? bs=4M status=progress를 입력한다. 기다리면 No space left on device라는 문구가 뜨며 완료된다.

[15] 만약 랜덤필->제로필->랜덤필을 하고 싶다면, 터미널에서 sudo dd if=/dev/urandom of=/dev/??? bs=4M status

=progress; sudo dd if=/dev/zero of=/dev/??? bs=4M status=progress; sudo dd if=/dev/urandom of=/dev/??? bs=4M status=progress 를 입력하면 된다. 시간이 좀 걸리므로 한숨 자면 된다.

[16] 노트북의 경우 노트북을 덮으면 진행이 멈추므로 완전 삭제 과정 중에는 노트북을 덮지 않는다.

[17] HDD/SSD 포맷하기 문단을 참고한다.

[18] 내장 SSD는 Trim과 Secure Erase라도 할 수 있지 외장 SSD, USB, SD카드는 그마저도 못하기 때문에 만약 처음 구입할 때부터 암호화해두지 않았다면 랜덤필 2번한 뒤 물리적으로 박살내는 것 말고는 답이 없다.

[19] 단 웨어레벨링이 완전삭제에 무조건 불리한 점만 있는 것은 아니다. 웨어레벨링 때문에 HDD와 달리 원본 데이터의 손실이 빨리 일어나기도 한다. 데이터 회전율이 높은 SSD는 몇 시간만 지나도 소프트웨어 단에서는 복구가 매우 힘들어진다.

[20] 추측일 뿐이므로 한 귀로 흘리는 것이 좋다. 공식 사이트 문서를 읽는 것이 가장 좋다.

[21] WINDOWS HOST OS ENCRYPTION부터 암호화 관련 내용이다.

[22] 16GB SD 카드에 16GB 용량의 데이터를 쓰려고 하는데 15GB에서 파일이 더 들어가지 않는다면 1GB 용량의 히든 볼륨이 존재한다고 유추하기 쉽다.

[23] 기록 거부: 구글 접속 후 로그인 > 하단 "설정" > 좌측 상단 "줄 세 개(햄버거 메뉴)" > "활동 제어" > 전부 일시 중지, 기록 삭제: 구글 접속 후 로그인 > 하단 "설정" > 좌측 상단 "줄 세 개(햄버거 메뉴)" > 날짜별 활동 삭제 > 전체 기간 > 삭제.

[24] 아이폰은 20자리 이상도 가능하므로 비밀번호 자릿수 제한 걱정은 안 해도 된다. 예를 들어 '종교사회학 광고주 갈매기 도미니카 공소시효 까막눈'을 비밀번호로 한다면 이 비밀번호는 58자리라서 Onu UI 5.0 이전의 안드로이드 스마트폰은 설정할 수 없지만 아이폰은 가능하다. 단 옛날 아이폰도 비밀번호 자릿수 제한이 없는지는 알 수 없는 상태.

[25] 메타데이터란 어떤 데이터를 설명해 주는 데이터를 말한다. 예를 들어 사진을 찍은 날짜와 시간, 사진을 찍은 스마트폰 모델명, 사진의 가로세로 크기, 사진의 위치정보 등은 사진에 대해 설명해 주고 누군가와 통화를 했을 때 누구와 통화했는지, 언제 통화했는지, 얼마나 오랫동안 통화했는지, 서로 얼마나 자주 통화하는지 등은 통화 내용에 대해 설명해 주는 게 메타데이터이다. 메타데이터라는 개념은 다양한 곳에 활용된다.

[26] 만약 토어 브라우저, VPN, 익명 메신저 등을 특별한 때에만 사용한다면 그 자체도 메타데이터가 될 수 있다. 그러므로 평범한 웹서핑을 할 때도 토어나 VPN을 쓰고 일반적인 대화를 할 때도 익명 메신저를 쓰는 것이 좋다.

[27] 사진에 대한 메타데이터로 EXIF를 들 수 있다.

[28] 윈도우에서 ExifCleaner를 쓰려는 경우 홈페이지에서 'Download for FREE'를 클릭한 뒤 'ExifCleaner-3.6.0.exe'나 'ExifCleaner-Setup-3.6.0.exe'를 클릭하여 파일을 다운받으면 된다.

[29] 참고로 마우스 움직이는 습관을 숨기는 방법은 현재로서는 토어 보안레벨 Safest가 최선이다.🔗#,🔗#

[30] 프로톤메일이 토어 Safest에서 사용 가능한 이메일보다는 못하지만 네이버메일, 카카오메일, 구글메일보다는 프로톤메일이 낫다. 보통은 편의성때문에 프로톤메일 정도에서 만족하는 경우가 많다.

[31] 참고로 gpg4usb라는 프로그램은 ECDSA/EdDSA(ed25519)를 지원하지 않는다. 그러므로 만약 상대방이 gpg4usb를 쓴다면 RSA 4096비트를 선택한다.

[32] 대다수 커뮤니티에서는 글자수 제한 때문에 이용하기 어려울 것으로 보인다.

[33] 이 글에서 Onion 이메일은 보이지 않는다.

[34] 참고로 정확하게는 몰라도 IRC, Matrix, XMPP라는 게 있구나라는 정도는 알아두면 좋다. IRC 클라이언트로는 Hex Chat 등이 있고, Matrix 클라이언트로는 Element, Nheko Reborn 등이 있고, XMPP 클라이언트로는 Dino IM, Gajim, Conversations 등이 있다.🔗# 셋 다 초보자에게 쉽지 않은 난이도와 불편한 사용감 때문에 한국인 이용자는 거의 없다. Element는 상대적으로 쉬운 난이도 덕분에 상황이 나은 편이다. 가족이나 친구에게 카카오톡을 대체할 메신저를 추천해 주고 싶다면 차라리 Signal, Session, Briar, SimpleXChat 등 다른 메신저를 추천해 주는 것이 훨씬 낫다.

[35] Session은 기반이 되는 Lokinet이 토어 네트워크만큼의 신뢰성를 갖추지 못했다는 점 등을 지적받았다.🔗#

[36] SimpleX Chat은 여러 문제점을 지적받았다.🔗# 만약 SimpleX Chat을 사용할 경우 메신저가 토어로만 연결되도록 설정(Use SOCKS proxy)하고 Orbot을 같이 사용해야 한다. 만약 영어를 못한다면 🔗여기를 참고할 수 있다.

[37] 이 글 하나만으로 IRC를 완전히 이해하는 것은 어려우므로 다른 정보글도 찾아 보는 것을 권한다.

[38] 이 글 하나만으로 XMPP를 완전히 이해하는 것은 어려우므로 다른 정보글도 찾아 보는 것을 권한다.

[39] 카카오톡은 한 사람만 다른 사람을 친구추가해도 메세지를 보낼 수 있지만 Briar는 두 사람 모두 서로를 친구추가해야 대화가 가능하다.

[40] 만약 Briar를 사용한다면 '해외직구 Pixel폰+GrapheneOS+Briar'가 가장 좋다. 만약 Pixel폰을 구하기 어렵다면 자급제 기기를 구매하여 통신사 앱을 설치하지 않도록 한다. 결제는 현금/Monero/Zcash가 좋고 현금의 경우 이동할 때 조심한다. 안드로이드폰을 2개 구하고 가족 및 친구와 소통하기 위한 Briar ID와 제3자와 소통하기 위한 Briar ID를 각각 분리한다. 연결 설정을 보면 '같은 와이파이 네트워크에 연결된 지인과 연결하기' 옵션이 켜져 있는데 이 옵션을 끈다. 특수한 상황(ex. 인터넷이 안됨)을 제외하면 평소에는 '같은 와이파이 네트워크에 연결된 지인과 연결하기' 옵션과 '블루투스로 지인과 연결하기' 옵션을 꺼둔다. '토어 네트워크 연결방식' 옵션은 '브리지를 통해 토어 네트워크 연결하기'로 변경한다. 보안 설정에서 '앱 잠금' 옵션을 켠다. 원거리에서 연락처 추가를 위한 링크(briar://어쩌고저쩌고)를 게시할 때는 PGP의 공개키와 마찬가지로 익명인 계정에서 게시하는 것이 좋다. 예를 들어 네이버 블로그에 Briar 링크를 게시하는 것은 권하지 않는다. Briar ID의 비밀번호와 스마트폰의 비밀번호는 20자리 이상으로 강력하게 만든다.🔗#🔗#🔗#🔗#

[41] Briar가 좋은 메신저는 맞지만 100% 완전무결한 메신저라고 생각하는 것은 금물이다. 세상에 완벽한 것은 존재하지 않는다.

[42] Briar는 상대방에게 내 기기의 블루투스 MAC 주소를 전송하므로 완전한 익명이 아니다. Briar는 대화의 내용과 메타데이터(상대방과 언제 대화하는지, 얼마자 자주 대화하는지 등)는 숨길 수 있지만 나와 상대방이 누구인지는 숨길 수 없다.🔗#

[43] 단 Cwtch는 아직 보안감사를 받지 않았으므로 2023년 6월 현재는 조금 신중할 필요가 있다.🔗#

[44] 단 Onion사이트는 HTTPS 없이도 자체적인 Onion 프로토콜로 종단 간 암호화를 지원하므로 HTTP라고 신경 쓰지 않아도 된다.

[45] 중간자 공격(man in the middle attack)에 대비하기 문단을 보면 된다.

[46] 탐정 신문의 탐정 셜록 시리즈의 일부 내용을 오프라인 프라이버시를 추구할 때 참고할 수 있다.(ex. 겉과 속의 무늬가 다른 양면옷 착용)

[47] 약 200편 정도이다. 다 읽을 필요는 없고 관심 있는 부분만 읽어도 된다.

[48] 21, 29, 47, 49편이다.

[49] 단 착신전환 기능을 이용해 익명으로 전화한다는 글에 대해서는 회의적이다.🔗#

[50] SDR(Surveillance Detection Route) 등 오프라인 프라이버시에 도움되는 내용이 들어있다.

[51] 특이하게도 목차가 맨 뒷쪽에 있다.

[52] ex. 야동사이트, 토토사이트 등

[53] Opening Posts만 검색한다.

[54] 모든 포스트를 검색한다.

[55] 2026년 6월 기준으로 클리어넷 사이트는 닫혀있고 onion 사이트만 열려있다.

[56] 단 구글 연관 검색어로 'The hitchhiker's guide to online anonymity is wildly inaccurate'가 있는 것을 보면 글에 틀린 내용이 섞여있을 수도 있으니 읽을 때 맹신하면 안 된다.

[57] 토어를 키고 들어가야 한다.

[58] 모질라 파이어폭스 포터블 버전을 토어에 맞게 수정하고 토어의 기본요소를 내장

[59] 이 링크엔 토어 외에도 쓸 수 있는 프록시 프로그램을 알려준다.

[60] 예를 들어 디시에서 토어로 접속한 뒤 유동닉 + 자짤 없음 + 흔하디 흔한 닉네임 + 아무렇게나 친 비밀번호를 사용한다면 단순 명예훼손/모욕죄로는 경찰이 수사를 하기 싫을 정도의 보안을 유지할 수 있지만 토어로 접속한 뒤 고정닉 아이디로 접속하거나 평소에 써 오던 고정닉 아이디 혹은 닉네임과 동일하게 정한 유동닉을 사용했다면 경찰 수사는 사실상 불가능에서 시간 문제로 바뀐다.

[61] 특히 네이버같이 실명인증이 필요한 사이트.

[62] https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea 2010년 포스팅한 글이다. 다만 포스팅 밑의 익명 댓글란에서도 P2P사용과 관련된 논의가 있었다.

[63] 그럼에도 많은 사람들이 이러한 목적으로 사용하며, 트래픽 상으로는 이러한 트래픽이 매우 높은 비중을 차지하는 것이 현실이다. 한국이 음란물이 금지되어 있다고 해도 아주 간단하게 우회하여 빠르게 이용할 수 있으므로, 토어를 이용해서 야동을 보려고 하는 사람들은 거의 100% 저런 경우에 해당한다.

[64] qbittorrent의 익명 모드가 P2P 핑거프린팅을 완벽히는 못해도 조금이나마 방어해 준다고 한다. 다만 완벽한 방어는 못하니 qbittorrent 익명모드와 유료VPN을 이용해 파일을 다운받은 뒤 바로 qbittorrent를 삭제하고 필요할 때만 다시 qbittorrent를 설치하는 것이 좋다.

[65] 혹시나해서 말하는데 토렌트로 아청물받을 생각은 추호도 하지 마라. 세상엔 똑똑한 경찰이 많다.

[66] Brave의 토어 기능을 사용하면 Brave 검색엔진으로 연결된다.

[67] 다만 역으로 피의자들이 핸드폰에 프로그램을 설치하지 않는다면 토어 자체로 추적하는 건 난이도가 높다는 방증이기도 하다.

[68] 사실 물리적 압수수색도 만만치 않다. 전체 디스크 암호화에 의해 간단히 무력화되기 때문이다. 전문 해커들은 소거 프로그램등으로 몇 번씩 하드 드라이브를 지워댈뿐만 아니라 그것과 같이 병행해서 디스크를 물리적으로 파괴하고 강한 자석을 사용하거나 아예 정보 손실시 복구할 수 있는 가망이 없는 SSD만을 사용하여 증거인멸에 매우 큰 노력을 하고 있다.

[69] 물론, 구버전의 소프트웨어를 사용하는 등의 실수가 있었다. 다만 프라이버시 보호를 위한 여러 행동 수칙을 완벽하게 지키는 것이 어려움을 고려하면, 충분히 괄목할 만한 사례이다.

[70] 해외 사이트에서 토어 없이 딱봐도 명예훼손이나 모욕죄로 걸릴 욕을 한 이용자를 경찰이 잡으려고 해도 잡지 못하는 이유가 국제공조가 안 되기 때문이다. 잡으려면 신원을 알아내야 하는데 국가기관도 아니고 사이트 운영자가 '우리 약관에는 그 정도 욕설한 걸로는 위반이 아니기에 정보를 넘겨 줄 수 없다'고 뻗대고, 애초에 해외에서는 한국의 명예훼손이나 모욕죄와 비슷할 정도로 말 한번 잘못했다고 바로 고소를 할 수 있는 법률이 없어서 그렇게 뻗댈 수 있는 것이다. 잡히는 경우는 욕을 한 사람이 자신이 어디사는 누구라고 신상을 뿌린 것을 피해자 본인이 정보를 수집해 수사기관에 넘겨서 걸린 경우이다. 그렇다고 절대 공조하는 일이 없는 것은 결코 아니다. 실제로 구글이나 유명 SNS에서는 이미 한국 수사기관의 요청에 따라 정보를 주고받고 있으며, 명예훼손 사안에 대해서도 그렇게 검거하여 처벌한 사례들이 여럿 있다. 다만 좀 심한 경우에만 해당된다는 것이다.

[71] 원래 토어는 이유가 국가기관의 인터넷 통제로 고통받는 사람들에게 **국가기관에 걸리지 않고** 하고 싶은 말과 정보를 제공할 수 있도록 안전하게 인터넷을 하기 위해 만들어진 프로그램이지 남에게 피해주는 불법적인 행위나 n번방 성착취물 제작 및 유포 사건 등 현실의 아동을 대상으로 촬영한 포르노나 보라고 만들어진 프로그램이 절대 아니다.

[72] 외국 사이트에 회원가입할 시에는 비밀번호는 한/영키를 영어로 하고 독도는 우리땅, 한국을 빛낸 100명의 위인들 등 노래 재목을 입력하면 영어로는 알아볼 수 없는 배열이 되기 때문에 기억하기 쉬우면서도 안전한 비번을 만들 수 있다.

[73] 기업들의 개인정보취급정책이나 도덕성을 전적으로 믿는다면 몰라도 이미 여러 사건들을 보고도 그럴 수 있을지...

[74] 일반채팅의 경우에는 종단 간 암호화 서비스를 제공하지 않는다.

[75] 원래는 클라이언트 쪽 암호화 방식으로 서비스를 제공하다가 2006년에 서버 쪽에서 암호화와 복호화를 진행하고 그 후 SSL로 유저에게 전송하는 방식으로 바꿔버렸다. 즉 Hushmail 측은 마음만 먹으면 얼마든지 볼 수 있다는 뜻이며 해커들도 취약점을 이용할 수 있다.

[76] 암호화와 복호화가 클라이언트가 아닌 서버 쪽에서 이루어졌고 그조차도 평문 상태의 비밀번호를 받아 이루어졌다. 이 말은 "암호화된 메일" + "복호화 키" + "복호화 키를 쓰는 데 필요한 비밀번호" 이 세 가지가 모두 서버에 저장되어 있다는 뜻이며(~~삼위일체~~) 이건 자물쇠와 열쇠를 한 곳에 두는 것이나 마찬가지다. 그런데도 이 업체는 '보안이 너무 확실해서 자신들조차 메일을 읽을 수 없다'고 메인페이지에 적어놓고 있었다. 물론 스노든 사건 이후 지금은 문 닫았다.

[77] 문서를 참고하면 알 수 있듯이 부모들한테는 좋지만 이것은 부당히 행복추구권을 침해받은 것이다.

이 문서의 내용 중 전체 또는 일부는 Tor(익명 네트워크) 문서의 r1290 판에서 가져왔습니다. 이전 역사 보러 가기

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.